Concept for Secure Banking Chip Coupled with Induction-Powered Microprocessor to Facilitate Improved Security Regime Based Upon Recursive HMAC-Based Changes to Stored Identifier in an Editable Chip

7 May 2024
Simon Edwards
Research Acceleration Initiative

Introduction

Although many have become familiar with the now-ubiquitous "chip cards" issued by banking institutions the world over, these chips, although more secure than a simple magnetic swipe in which plaintext card information must be stored, have proven to be vulnerable. These chips work by transmitting encrypted versions of card information through a reader which relays that information to the company that manufactured the card in order to perform authentication. As this encryption is based upon an open-key scheme, non-trivial cryptographic weaknesses exist which may be used to ascertain genuine card information through access to compromised encrypted data. The chips, themselves, also open the door to short-range radio-based theft of the encrypted version of the identifiers.

Abstract

A superior security regime is possible for banking applications through the addition of an induction-powered microprocessor which would be capable of interpreting inputs and performing modifications to the stored encrypted identifiers based upon purchase history. In this regime, purchase history would not be stored on the card but would be stored only by the bank and the credit card manufacturer. However, unique particulars of purchase history would be used in order to permute the stored identifiers.

Each time the encrypted identifier is read by a card reader and an authentic purchase is made, the unique encrypted identifier of the card changes, overwriting the previous identifier. The particular way in which the identifier is altered would be based upon an HMAC function in which the date and time of the transaction along with a confidential code unique to the merchant. As the bank and the credit card company would know of these confidential codes and the dates and times of all users' historical purchases, they would have sufficient information to determine what unique identifier would be valid for the next purchase. As the stored identifier would be physically altered in the memory of the chip as a consequence of being inserted into a card reader and a transaction being successfully completed, an entirely different encrypted identifier would be transmitted by subsequent merchants and the compromise of one merchant's database would not enable a malicious party to succeed in executing a transaction.

The simple addition of a unique private key (unique to each card) which would perform an additional encrypting pass after the HMAC step would ensure that the value to which the identifier is changed would remain unknown to any party except for the credit card company/authenticator.

Conclusion

The private key would be physically prohibited from being leaked through exploit attempts and could only be applied to the internal alteration of the authenticator.